UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/813,248	03/30/2004	Plinio Pimentel	3408.2.8	4822

21552 7590 10/20/2008

MADSON & AUSTIN
15 WEST SOUTH TEMPLE
SUITE 900
SALT LAKE CITY, UT 84101

EXAMINER	
OKEKE, IZUNNA	
ART UNIT	**PAPER NUMBER**
2432	
MAIL DATE	**DELIVERY MODE**
10/20/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/813,248	PIMENTEL, PLINIO	
	Examiner	Art Unit	
	IZUNNA OKEKE	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *30 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *07/02/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Vainstein (US-6889210).

a. *Referring to claim 1:*

Regarding claim 1, Vainstein teaches in a computing device, a method for protecting sensitive files from unauthorized access (Col 4, Line 26-58 teaches a method for protecting sensitive and confidential files from unauthorized access), comprising:

detecting a connection of the computing device to an electronic device; accessing an authorized connection list (Col 5, Line 35-67 and Col 6, Line 1-23 teaches a user or device connecting to a system holding electronic data wherein a list denotes an access list and rules for authorized users);

determining whether the connection is identified in the authorized connection list; and

if the connection is not identified in the authorized connection list: accessing sensitive file information which identifies at least one sensitive file stored on the computing device; and

preventing access to the at least one sensitive file identified by the sensitive file information (Col 6, Line 9-23 teaches ensuring that only authorized clients can access the confidential files and if

the client is unauthorized or doesn't have the level of trust, preventing access to the files by the users).

a. *Referring to claim 2:*

Regarding claim 2, Vainstein teaches the method of claim 1, wherein if the connection is not identified in the authorized connection list the method further comprises: detecting termination of the connection; and if the computing device does not have any other unauthorized connections, restoring access to the at least one sensitive file identified by the sensitive file information (Col 6, Line 8-67 teaches access lists and levels of access wherein if a user is not identified in the list, the system restricts access to the sensitive devices but allows access when a user is an authorized user).

a. *Referring to claim 3:*

Regarding claim 3, Vainstein teaches the method of claim 1, wherein the connection occurs via a computer network (Col 1 and 2 teaches a network connection over the internet).

a. *Referring to claim 4:*

Regarding claim 4, Vainstein teaches the method of claim 3, wherein the network is a wireless network, and wherein the computing device is a mobile computing device (Col 5, Line 49-52 teaches the client as a device such as a mobile device as is known in the art).

a. *Referring to claim 5:*

Regarding claim 5, Vainstein teaches the method of claim 1, wherein the connection is a direct connection (Col 1 and 2 teaches a direct connection between a client and file storage system in an intra-corporation network).

a. *Referring to claim 6:*

Regarding claim 6, Vainstein teaches the method of claim 1, wherein preventing access to the at least one sensitive file comprises locking the at least one sensitive-file (Col 5, Line 63-67 and Col 6, Line 1-8 teaches locking the files to protected with a file key).

a. *Referring to claim 7:*

Regarding claim 7, Vainstein teaches the method of claim 1, wherein preventing access to the at least one sensitive file comprises encrypting the at least one sensitive file (Col 5, Line 63-67 teaches securing the files by encrypting them).

a. *Referring to claim 8:*

Regarding claim 8, Vainstein teaches the method of claim 1, wherein the computing device comprises a storage device, and wherein preventing access to the at least one sensitive file comprises moving the at least one sensitive file to a host-protected area of the storage device (Col 5, Line 63-67 teaches another way of protecting the files by writing it into a store or protected storage).

a. *Referring to claim 9:*

Regarding claim 9, Vainstein teaches the method of claim 1, wherein the sensitive file information is a reference to a directory in which the at least one sensitive file is stored (Col 7, Line 17-31 teaches a header file structure linked to the protected files which references or points to the location of the protected file).

a. *Referring to claim 10:*

Regarding claim 10, Vainstein teaches the method of claim 1, wherein the sensitive file information is a list of the at least one sensitive file (Col 7, Line 17-31 teaches a header file structure linked to the protected files which lists the sensitive file and its level of protection).

a. *Referring to claim 11:*

Regarding claim 11, Vainstein teaches the method of claim 1, wherein the authorized connection list comprises a list of at least one authorized network (Col 6, Line 9-15 teaches an access list which comprises a list of who should access the files).

a. *Referring to claim 12:*

Regarding claim 12, Vainstein teaches the method of claim 1, wherein the authorized connection list comprises a list of at least one authorized connection type (Col 6, Line 9-23 teaches an access rules list which comprises a list of who should access the files and the access rules for the user).

a. *Referring to claim 13:*

Regarding claim 13, Vainstein teaches In an administrative system which distributes software to a plurality of computing devices on an enterprise network, a method comprising: providing a security agent, wherein after installation on a computing device the security agent is configured to implement a method comprising (Col 4, Line 26-47 teaches security parameters and software products configured on a computing device to implement the method of safeguarding confidential information) :

detecting a connection of the computing device to an electronic device; accessing an authorized connection list; determining whether the connection is identified in the authorized connection list (See the rejection in claim 1);

and if the connection is not identified in the authorized connection list: accessing sensitive file information which identifies at least one sensitive file stored on the computing device (See the rejection in claim 1); and

preventing access to the at least one sensitive file identified by the sensitive file information; and transmitting the security agent to the plurality of computing devices via the enterprise network (See the rejection in claim 1).

a. *Referring to claim 14:*

Regarding claim 14, Vainstein teaches the method of claim 13, further comprising: providing the authorized connection list; providing the sensitive file information; and transmitting the authorized connection list and the sensitive file information to the plurality of computing devices via the enterprise network (Col 6, Line 9-34 teaches the security information, the access list and access rules list which is maintained by the computing devices housing the sensitive data).

a. *Referring to claim 15:*

Regarding claim 15, Vainstein teaches a computing device that is configured for protecting sensitive files from unauthorized access, comprising: a processor; memory in electronic communication with the processor (Col 4, Line 25-67 teaches a system configured for protecting sensitive files and as is known in the art such systems comprises a processor and memory); and

instructions stored in the memory, the instructions being executable to implement a method comprising: detecting a connection of the computing device to an electronic device; accessing an authorized connection list; determining whether the connection is identified in the authorized connection list (See the rejection in claim 1);

and if the connection is not identified in the authorized connection list: accessing sensitive file information which identifies at least one sensitive file stored on the computing device (See the

rejection in claim 1); and

preventing access to the at least one sensitive file identified by the sensitive file information (See the rejection in claim 1).

a. *Referring to claim 16:*

Regarding claim 16, Vainstein teaches the computing device of claim 15, wherein if the connection is not identified in the authorized connection list the method further comprises: detecting termination of the connection; and if the computing device does not have any other unauthorized connections, restoring access to the at least one sensitive file identified by the sensitive file information (See the rejection in claim 2).

a. *Referring to claim 17:*

Regarding claim 17, Vainstein teaches the computing device of claim 15, wherein preventing access to the at least one sensitive file comprises at least one of locking the at least one sensitive file, encrypting the at least one sensitive file, and moving the at least one sensitive file to a host-protected area of a storage device (See the rejections in claims 6, 7 and 8).

a. *Referring to claim 18:*

Regarding claim 18, Vainstein teaches a computer-readable medium for storing program data, wherein the program data comprises executable instructions for implementing a method comprising (Col 4, Line 1-58 teaches a software product for performing the methods of data protection and it is known in the art for these software products to comprise instructions or program data embodied on a computer readable medium):

detecting a connection of a computing device to an electronic device; accessing an authorized connection list; determining whether the connection is identified in the authorized connection

list; and if the connection is not identified in the authorized connection list (See the rejection in clam 1):

accessing sensitive file information which identifies at least one sensitive file stored on the computing device; and preventing access to the at least one sensitive file identified by the sensitive file information (See the rejection in claim 1).

a. *Referring to claim 19:*

Regarding claim 19, Vainstein teaches the computer-readable medium of claim 18, wherein if the connection is not identified in the authorized connection list the method further comprises: detecting termination of the connection; and if the computing device does not have any other unauthorized connections, restoring access to the at least one sensitive file identified by the sensitive file information (See the rejections in claims 2 and 18).

a. *Referring to claim 20:*

Regarding claim 20, Vainstein teaches the computer-readable medium of claim 18, wherein preventing access to the at least one sensitive file comprises at least one of locking the at least one sensitive file, encrypting the at least one sensitive file, and moving the at least one sensitive file to a host-protected area of a storage device (See the rejections in claims 6, 7 and 8 and 18).

Conclusion

3. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Bhogal et al. (US-2004/0003289) discloses a method, apparatus, and computer instructions for managing files in a data processing system. (See Abstract)

a. Elliot et al (US-2003/0056095) discloses a method, system and computer program product for securing decrypted files in a shared environment.

a. Dorn et al. (US-20040153675) discloses the invention concerns a procedure for logging a user into a data processing device with an operating system and a data processing program. (See Abstract)

Any inquiry concerning this communication or earlier communications from the examiner should be directed to IZUNNA OKEKE whose telephone number is (571)270-3854. The examiner can normally be reached on 9:00am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/I. O./
Examiner, Art Unit 2432

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2432